PATENT ABSTRACTS OF JAPAN

(51)Int.Cl.   H04L   9/32
                               G06F 15/00
                               H04L   9/08
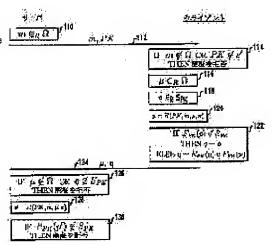
(54) MUTUAL NETWORK AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a password single mutual authentication protocol which can prove safety.

SOLUTION: A client decides whether a public key received from a server is the element of the test possible super set of the set of all public keys in a public key cipher system. When it is not such element, authentication is refused by the client. If not, a protocol is continued. In one embodiment, the client and the server shares one password used for authentication. The client generates a parameter (p) as the function of at least the public key and the password. When, as a result of operating a public key space mapping function FPK to (p), the FPK is the element of the message space of the public key, the client uses the open key to cipher the substantially random element in the message space of the public key and executes the group operation of the public key message space between the ciphered result and the FPK (p).

(54)【発明の名称】 相互ネットワーク認証方法

サーバ クライアント

$m \in_R \Omega$ 〜110

m, PK 〜112

IF $m \notin \Omega$ OR $PK \notin \varepsilon'$ THEN 認証を拒否 〜114

$\mu \in_R \Omega$ 〜116

$\sigma \in_R S_{PK}$ 〜118

$p = H(PK, m, \mu, \pi)$ 〜120

IF $F_{PK}(p) \notin S_{PK}$ THEN $q = a$ ELSE $q = E_{PK}(a) \circ F_{PK}(p)$ 〜122

μ, q 〜124

IF $\mu \notin \Omega$ OR $q \notin S_{PK}$ THEN 認証を拒否 〜126

$p' = H(PK, m, \mu, \pi)$ 〜128

IF $F_{PK}(p') \notin S_{PK}$ THEN 認証を拒否 〜130